SPW2137

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	LOTSPIECH	Art Unit:	2137
Serial No.:	09/771,239	Examiner:	Z. Davis
Filing Date:	January 26, 2001		**Docket#:ARC920010006US1**
For:	METHOD FOR TRACING TRAITOR RECEIVERS IN A BROADCAST ENCRYPTION SYSTEM		September 20, 2004 750 "B" Street, Suite 3120 San Diego, CA 92101

TRANSMITTAL LETTER AND SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
Alexandria, VA 22313

Dear Sir:

Pursuant to Sections 1.97, 1.98, and 1.99 of the Rules of Practice in patent cases, copies of the references cited on the "List of References Cited by Applicant," Form PTO-1449 are submitted herewith. An acknowledgment postcard is also enclosed.

The Commissioner is authorized to charge $180 to Deposit Account 09-0441 for the Information Disclosure fee.

Respectfully submitted,

John L. Rogitz
Attorney of Record
Registration No. 33,549
750 "B" Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR/jg
Encs.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service, First Class Mail, postage fully prepaid, under 37 CFR 1.8, addressed to MAIL STOP AMENDMENT Commissioner for Patents, Alexandria, VA 22313 on SEPTEMBER 21, 2004.

Date Signed: SEPTEMBER 21, 2004

JEANNE GAHAGAN

Form PTO-1449 (modified)	Attorney Docket No. ARC920010006US1	Serial No. 09/771,239
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT(S)' INFORMATION DISCLOSURE STATEMENT *(Use several sheets if necessary)*	Applicant(s):	LOTSPIECH et al.
	Filing Date: 01/26/2001	Group Art Unit: 2137

U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
	US2002/0090090 A1	07/11/2002	Van Rijnsoever et al.	380	279	
	6,397,329 B1	05/28/2002	Aiello et al.	713	155	
	6,684,331 B1	01/27/2004	Srivastava	713	163	

PUBLICATIONS / OTHER ART

Examiner Initials	Citation
	PUBLICATION: "Secure Group Communications Using Key Graphs". Wong et al. Proceedings of ACM SIGCOMM. Pgs 1-12. September, 1998. Canada.
	PUBLICATION: "Efficient Communication-Storage Tradeoffs for Multicast Encryption". Canetti et al. EUROCRYPT 1999. Pgs. 459-474.
	PUBLICATION: "Key Establishment in Large Dynamic Groups Using One-Way Function Trees". McGrew et al. Submitted to IEEE Transactions on Software Engineering. Pgs. 1-13. May, 1999.
	PUBLICATION: "Multicast Security: A Taxonomy and Some Efficient Constructions". Canetti et al. Proc. of INFOCOM. Vol. 2, pp. 708-716. New York, March 1999.
	PUBLICATION: "Broadcast Encryption". CRYPTO 1992, LNCS Vol. 839, pp. 257-270, New York, March 1994.

Examiner Date Considered

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance *and* not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449 (modified)	Attorney Docket No. ARC920010006US1	Serial No. 09/771,239
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT(S)' INFORMATION DISCLOSURE STATEMENT	Applicant(s):	LOTSPIECH et al.
(Use several sheets if necessary)	Filing Date: 01/26/2001	Group Art Unit: 2137

U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
	5812670	09/22/1998	Micali	380	25	
	5675649	10/07/1997	Brennan et al.	380	21	
	5748736	05-1998	Mittra	713	163	
	6629243	09-2003	Kleinman	713	163	
	6247127	06-2001	Vandergeest	713	100	
	6285991	09-2001	Powar	705	76	
	5241597	08/31/1993	Bright	380	21	

PUBLICATIONS / OTHER ART

Examiner Initials	Citation
	PUBLICATION: "Sequential Traitor Tracing". R. Safavi-Naini and Y. Wang. CRYPTO 2000, LNCS vol. 1880, PP. 316-332, 2000.
	PUBLICATION: "Efficient Trace and Revoke Schemes". M. Naor and B. Pinkas. Financial Cryptography '2000, LNCS 1962, pp. 1-20, 2001.
	PUBLICATION: "Efficient Methods for Integrating Traceability and Broadcast Encryption". E. Gafni, Jessica Staddon and Yiqun Lisa Yin. CRYPTO '99, Springer-Verlag LNCS 1666, pp. 372-387, 1999.
	PUBLICATION: "Trials of Traced Traitors". Birgit Pfitzmann. Workshop on Information Hiding, Cambridge, UK, LNCS, Vol. 1174, Springer-Verlag, pp. 1-16, 1996.
	PUBLICATION: "Digital Signets: Self-Enforcing Protection of Digital Information". C. Dwork, J. Lotspiech and M. Naor. 28th Symposium on the Theory of Computation, pp. 489-498, 1996.
	PUBLICATION: "An Efficient Public Key Traitor Tracing Scheme". D. Boneh and M. Franklin, Proceedings CRYPTO '99, LNCS, Vol. 1666, Springer-Verlag, pp. 1-13, i-iv, 1999.

	PUBLICATION: "Collusion-Secure Fingerprinting for Digital Data". D. Boneh and J. Shaw. IEEE Transactions on Information Theory, Vol. 44, No. 5, pp. 1897-1905, 1998.
	PATENT APPLICATION: "Forensic Media Key Block for Identifying Compromised Keys". Lotspiech. Co-pending application serial no. 09/564,658, filed May 3, 2000.
	PUBLICATION: "Threshold Traitor Tracing". M. Naor and B. Pinkas, CRYPTO '98, LNCS vol. 1462, pp. 502-517, 1998.
	PUBLICATION: "Efficient Dynamic Traitor Tracing". O. Berkman, M. Parnas and J. Sgall. Proceedings of the 11th ACM-SIAM Symp. On Discrete Algorithms (SODA), PP. 586-595, 2000.
	PUBLICATION: "Tracing Traitors". B. Chor, A. Fiat, M. Naor and B. Pinkas. IEEE Transactions on Information Theory, Vol. 46, No. 3, May 2000.
	REPORT: "Key Management for Multicast: Issues and Architectures". D. Waller, E. Harder, and R. Agee. National Security Agency, pp. 1-19, June 1999.
	PUBLICATION: "On the Generation of Cryptographically Strong Pseudorandom Sequences". Adi Shamir, ACM Transactions on Computer Systems, vol. 1, no. 1, pp. 38-44, February 1983.
	PUBLICATION: "Tracing Traitors". B. Chor, A. Fiat and M. Naor. CRYPTO '94, Incs Vol. 839, pp. 257-270, 1994.

Examiner Date Considered

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance *and* not considered. Include copy of this form with next communication to applicant(s).